C-ISMS-DOC-05-2

[Restricted]

CBL Information Security Roles, Responsibilities and Authorities

Version 1.0

7th February 2025

CBL Information Security Roles, Responsibilities and Authorities

[Confidential}

Document Reference

Document Code:	C-ISMS-DOC-05-2
Document title:	CBL Information Security Roles, Responsibilities and Authorities
Filename:	C-ISMS-DOC- 05-2 Information Security Roles, Responsibilities and Authorities
Author:	Consultant
Owner:	CBL
Date:	7th February 2025
Version:	1.0
Status:	Final

Revision Record

Version	Date	Summary of Changes	Revision Author
1.0 Draft 1	11th December 2024	Establishment of Information Security Roles, Responsibilities and Authorities	Consultant
1.0 Draft 2	7th February 2025	Revision to align with PCI DSS v4.0; Assignment of PCI DSS responsibilities to CTO and employees.	CBL
	6th February 2026	Next Version	

Distribution

Name	Title
Alex Iwobi	Chairman
Francisca Ordega	Chief Executive Officer
Sopade Adeola	Chief Information Security Officer
Ngozi Okobi	Chief Technology Officer
Rasheedat Ajibade	ISMS Manager

CBL Information Security Roles, Responsibilities and Authorities

[Confidential}

Approval

Name	Position	Signature	Date
Alex Iwobi	Chairman		11 February, 2025
Sopade Adeola	Chief Information Security Officer		11 February, 2025

[Confidential}

Contents

[Confidential}

1. Introduction

1.1 Purpose and Alignment with ISO/IEC 27001

CBL treats the security of its information assets, payment systems, and customer data as a critical business priority. To support this, CBL has established an Information Security Management System (ISMS) aligned with the requirements of the ISO/IEC 27001 international standard. A key element of an effective ISMS is the clear definition and assignment of information security roles, responsibilities, and authorities to appropriate individuals and functions within the organisation.

1.2 Applicability and Supporting ISMS Documents

All employees, contractors, and relevant third parties are required to understand their role within the ISMS and their responsibility for protecting the information entrusted to CBL. This document should be read in conjunction with other ISMS documentation, including:

- Information Security Context, Requirements and Scope
- Information Security Management System Policy

1.3 Importance of Defined Security Responsibilities

Clearly defined roles and responsibilities enable CBL to proactively prevent information security incidents and to respond promptly and effectively when incidents occur.

1.4 Shared Responsibility in Cloud Operations

As CBL operates its core payment infrastructure within a cloud-based environment, this document also clarifies the shared responsibility model between CBL and its cloud service providers. This ensures that critical security activities, such as access control, monitoring, backup, and vulnerability management, are clearly owned and consistently performed.

2. Information Security Roles

2.1 Defined Roles

Within the ISMS, the following major roles need to be defined and allocated:

- Information Security Steering Committee
- Chief Information Security Officer
- Chief Technology Officer
- Information Asset Owner
- Information Security Risk Owner
- Information Security Auditor

2.1.1

The detailed responsibilities and authorities associated with each of these roles are defined in subsequent sections of this document.

2.1.2

In addition to the roles listed above, certain information security responsibilities are embedded within existing operational roles across CBL. These responsibilities are summarised in this document to ensure clarity and accountability.

2.1.3 Operational Roles

These operational roles include:

- Heads of Department
- IT and Engineering Team
- All Users (employees and contractors)

2.1.4

General information security responsibilities applicable to all employees, contractors, and relevant third parties are defined within CBL's information security policies and related procedures.

2.2 ISMS Responsibility Matrix

Overall responsibility for managing the requirements of the ISO/IEC 27001 standard at CBL is defined in the RACI matrix below. The matrix clarifies each role's level of involvement as follows:

R = Responsible | A = Accountable | C = Consulted | I = Informed

ISO/IEC 27001 Area	Information Security Steering Committee	Chief Technology Officer	Information Security Auditor
Context	A	C	I
Leadership	A	R	I
Planning	A	R	I
Support	A	R	I
Operation	A	R	I
Performance Evaluation	A	R	R

Improvement	A	R	R
Annexe A Controls	A	R	I

Table 1 – RACI Chart

The responsibilities outlined above reflect CBL's operating model, where governance and oversight are provided by management, while day-to-day implementation and operation of information security controls are led by the CTO, with independent assurance provided by the Information Security Auditor.

These responsibilities are described in more detail in the subsequent sections of this document.

3. Specific Role Responsibilities

This section defines the specific information security responsibilities and authorities assigned to each role within CBL's organisational structure. The responsibilities described here relate solely to information security and the operation of the ISMS and do not replace or duplicate general managerial, technical, or operational job responsibilities.

The competencies and skills required to perform each information security role effectively are defined in the ISMS document *Information Security Competence Development Procedure*.

3.1 Information Security Steering Committee

The Information Security Steering Committee provides oversight of CBL's ISMS on behalf of top management and holds overall accountability for its effectiveness and alignment with business and regulatory requirements.

3.1.1 Members

The committee is composed of members of CBL's senior management and includes, at a minimum:

- Chief Executive Officer (CEO)
- Chief Information Security Officer
- Chief Technology Officer (CTO)

3.1.1.1

Additional members may be appointed by the committee as required, based on business, regulatory, or security needs.

3.1.2 Responsibilities

The Information Security Steering Committee is responsible for:

- Establishing and approving CBL's information security policy, objectives, and ISMS plans.
- Promoting the importance of information security and continual improvement across the organisation.
- Ensuring information security requirements are identified and met to protect CBL, its customers, and partners.
- Providing oversight of information security risks affecting CBL's payment systems and services.
- Ensuring adequate resources are allocated to implement, operate, and improve the ISMS.
- Reviewing ISMS performance, audit results, and key security metrics at planned intervals.
- Reviewing significant information security incidents and approving corrective actions.
- Ensuring that third-party access to CBL systems and data is governed by appropriate contractual and security controls.

3.1.3 Authorities

The Information Security Steering Committee is authorised to:

- Approve significant information security-related expenditures.
- Authorise the allocation or recruitment of resources required to manage information security.
- Direct and escalate major information security incidents and response activities.

3.2 Chief Technology Officer

The Chief Technology Officer (CTO) is the primary role responsible for the day-to-day management and implementation of information security at CBL. The role combines technical leadership with responsibility for operating and maintaining security controls that protect CBL's payment systems, infrastructure, and customer data.

3.2.1 Responsibilities

The Chief Technology Officer is responsible for:

- Reporting information security matters, risks, and incidents to the Information Security Steering Committee on a regular and ad-hoc basis.

- Implementing and enforcing CBL's information security policies, procedures, and technical controls.
- Managing access to CBL systems, including user provisioning, privilege management, and periodic access reviews.
- Ensuring security controls are implemented, documented, and maintained across infrastructure and applications.
- Identifying, managing, and coordinating the response to information security incidents in line with defined procedures.
- Monitoring and reporting on security incidents, vulnerabilities, and control effectiveness.
- Defining annual information security improvement plans and tracking progress against agreed targets.
- Maintaining a continual improvement action log and reporting status to management.
- Participating in ISMS management reviews and internal audits.
- Providing security guidance and awareness to staff, including technical and operational security practices.
- Overseeing the protection of cardholder data and supporting ongoing PCI DSS compliance activities.
- Coordinating vulnerability scanning, penetration testing, and remediation activities in line with PCI DSS and ISMS requirements.
- Managing day-to-day technical security controls, including:
    - Access control and identity management
    - Patch and vulnerability management
    - Firewall, IDS/IPS, and network security controls
    - System hardening and secure configuration
    - Cryptographic key management
    - Logging and monitoring
- Acting as Information Asset Owner for assigned information assets, including maintaining asset records and participating in risk assessments.
- Identifying and addressing applicable regulatory, contractual, and technical compliance requirements.

3.2.2 Authorities

The Chief Technology Officer has the authority to:

- Declare and escalate information security incidents.
- Review and assess the effectiveness of security controls across all business areas.
- Take immediate action to prevent, contain, or mitigate information security incidents.
- Maintain information security records and documentation in accordance with ISMS and PCI DSS requirements.

3.3 Information Asset Owner

The Information Asset Owner is accountable for the secure and appropriate use of one or more information assets owned or managed by CBL, as recorded in the Information Asset Inventory. Information assets may include applications, databases, systems, documentation, and customer or transaction data.

3.3.1 Responsibilities

The Information Asset Owner is responsible for:

- Owning and overseeing the protection of assigned information assets.
- Ensuring appropriate security controls are implemented and reviewed for allocated assets.
- Participating in risk assessments related to assigned assets.
- Ensuring asset records and classifications are accurate and kept up to date in the asset inventory.

3.3.2 Authorities

The Information Asset Owner has the authority to:

- Request or approve the implementation of security controls for information assets under their ownership.

3.4 Information Security Risk Owner

The Information Security Risk Owner is accountable for the management of one or more information security risks identified within CBL's risk register and defined in the Risk Treatment Plan.

3.4.1 Responsibilities

The Information Security Risk Owner has the following responsibilities:

- Monitoring and managing assigned information security risks throughout their lifecycle.

- Ensuring that appropriate controls are implemented and reviewed to treat assigned risks.
- Participating in risk assessments and reviews relating to owned risks.
- Coordinating with Information Asset Owners and other stakeholders affected by the risks.

3.4.2 Authorities

The Information Security Risk Owner has the authority to:

- Escalate risks to management where treatment actions are insufficient or delayed.
- Approve residual risk levels following the implementation of agreed risk treatment actions, in line with CBL's risk appetite.

3.5 Information Security Auditor

The Information Security Auditor is responsible for fulfilling CBL's internal audit requirements under ISO/IEC 27001 and applicable supporting standards. The role provides independent assurance that the ISMS is effectively implemented, maintained, and operating as intended.

3.5.1 Responsibilities

The Information Security Auditor is responsible for:

- Planning, establishing, and maintaining the ISMS internal audit programme, including audit scope, criteria, methods, and frequency.
- Conducting internal audits at planned intervals to assess ISMS conformity and effectiveness.
- Ensuring audits are performed in an objective, independent, and impartial manner.
- Reporting audit findings, nonconformities, and improvement opportunities to relevant management.
- Maintaining documented audit records and evidence in line with ISMS requirements.
- Supporting preparation for ISO 27001 certification and surveillance audits.

3.5.2 Authorities

The Information Security Auditor has the authority to:

- Review and assess information security controls, processes, and procedures across CBL.
- Raise audit findings and report results directly to management for action and follow-up.

4. Other Roles with Information Security Responsibilities

There are a number of other internal roles within the organisation which, whilst not solely dedicated to information security, have relevant responsibilities and authorities.

4.1 Heads of Department

Heads of Department oversee operational units within CBL.

4.1.1 Responsibilities

Heads of Department are responsible for:

- Ensuring employees under their supervision have the necessary competencies and training to perform their roles securely.
- Communicating the importance of information security and how individual activities contribute to CBL's security objectives.

4.1.2 Authorities

Heads of Department have the authority to:

- Organise training and awareness activities for their teams, within budget.
- Take action to prevent or contain information security incidents within their area of responsibility.

4.2 IT and Engineering Team

The IT and Engineering Team plays a critical role in CBL's ISMS, providing technical expertise and operational support to maintain secure and reliable payment systems.

4.2.1 Responsibilities

The IT and Engineering Team is responsible for:

- Operating key IT processes, including incident and change management.
- Implementing and maintaining technical information security controls.
- Providing system administration services, such as user account management, backups, and patching.
- Monitoring networks and systems for security events, vulnerabilities, or intrusions.
- Supporting risk assessments and remediation actions for IT-related risks.

4.2.2 Authorities

The IT and Engineering Team has the authority to:

- Take immediate action to prevent, contain, or mitigate information security incidents within their scope of responsibility.

4.3 All Users

All CBL employees, contractors, and relevant third parties who access IT systems or information have responsibilities for maintaining information security. Detailed obligations are defined in CBL policies, such as the Acceptable Use Policy, and are summarised here.

4.3.1 Responsibilities

All Users are responsible for:

- Complying with CBL's information security policies, procedures, and standards relevant to their role.
- Reporting any actual or suspected information security incidents or vulnerabilities promptly.
- Participating in risk assessments or security exercises when requested.

4.3.2 Authorities

All Users have the authority to:

- Take immediate action to prevent, contain, or escalate information security incidents within their area of responsibility.

This document will be reviewed annually to ensure continual improvement of ISMS and PCI DSS.